IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA v. JEREMY HACHEY	CRIMINAL NO. 16-0128

MEMORANDUM

SCHMEHL, J. **March 7, 2017**

This case is one of numerous criminal prosecutions across the country that grew out of the government's investigation of a child pornography website. Because the site was on the dark web and was accessed using software that blocks ordinary means of identifying visitors, the FBI used a special method in which software essentially infiltrated visitors' own computers and caused them to report identifying information to the FBI. The FBI used this method pursuant to a warrant issued by a magistrate judge in Virginia even though many of the site visitors, including Defendant, were located in other districts. Defendant argues that the warrant thus exceeded the Virginia magistrate's authority, and the evidence against him should be suppressed. Courts handling other cases related to the same investigation have decided the issue in varying ways. Judge Pappert of this Court concluded there were several alternative reasons to deny suppression in *United States v. Werdene*, 188 F. Supp. 3d 431 (E.D. Pa. 2016). The undersigned's decision differs in some respects but agrees with the conclusion that suppression is neither required nor appropriate, and the motion will be denied.

Factual and Procedural Background

Playpen, also called "Website A" or "TARGET WEBSITE" in some filings, was a site on the dark web consisting of a forum dedicated to child pornography. More than 200,000 users advertised, distributed, and accessed images and videos of child pornography and engaged in discussion related to child pornography and the sexual exploitation of children. The FBI was able to find the server hosting Playpen in North Carolina. Agents seized the site and, in order to identify users, rather than simply shutting it down, they began hosting the site themselves from a government facility in the Eastern District of Virginia.

Identifying the users, however, was not possible with the usual investigative process, which would normally involve checking the server's records of the IP addresses of visitors to the website and then obtaining identifying information from the internet service providers ("ISPs") associated with those IP addresses. Playpen operated on the Tor network, accessible only using the Tor browser. Tor software obscures users' IP addresses by routing communication through a series of nodes. Essentially, an individual user's IP address is only sent to the first computer in the relay chain, not to the actual site the user visits, and thus cannot be discovered by working backward from the visited site's server; therefore, even while running Playpen's server themselves, agents were unable to learn the actual users' IP addresses through ordinary means.

To uncover the identities of Playpen visitors in the face of Tor's anonymity protections, the FBI sought to use a special Network Investigative Technique ("NIT"). With the NIT in place, when a visitor logged in to Playpen, "additional computer

instructions" would piggyback on the ordinary website content being sent to the visitor. Once downloaded to the visitor's computer, those instructions would cause the visitor's computer to send identifying information to a government-controlled receiving computer. The information the visitor's computer would send included: the computer's IP address, along with an associated date and time; a special identifying code to distinguish each visitor's computer; the type, version, and architecture of the computer's operating system; and the computer's Host Name, operating system username, and Media Access Control ("MAC") address, all used in identifying the computer. Once the visitor's computer has been made to send this information to the government, agents can figure out the visitor's identity.

While operating Playpen from the Eastern District of Virginia, the FBI applied to a United States Magistrate Judge in that district for a warrant to utilize the NIT. The application was supported by the thirty-one-page affidavit of Special Agent Douglas Macfarlane, including about four pages describing the operation of the NIT. The affidavit noted that the additional computer instructions would be downloaded to the visitors' own computers; that Playpen visitors used Tor to protect their anonymity; that Playpen had been run on a server in Lenoir, North Carolina, and administered by a resident of Naples, Florida; and that the point of the warrant was to identify and locate Playpen users. The magistrate issued the warrant on February 20, 2015.

Using the NIT, agents learned the IP address and other identifying information for the computer of Playpen user "DalphonTheGreat," who had accessed particular posts on the site that contained child pornography; with the IP address known, they were able to use normal investigative procedures to discover Defendant's location and identity from

his ISP. On the basis of that information, which identified Defendant, with an address in Lititz, Pennsylvania, a magistrate judge in this district issued a warrant to search the defendant's home. On December 15, 2015, agents found an encrypted hard drive in Defendant's bedroom and elicited Defendant's admissions that he had downloaded child pornography and that his hard drive contained many child pornography files.

Defendant was subsequently indicted on March 31, 2016, on one count of receipt of child pornography under 18 U.S.C. § 2252(a)(2) and one count of possession of child pornography under 18 U.S.C. §2252(a)(4)(B). Defendant then filed a motion to suppress all evidence seized during the December 15, 2015, search, along with any admissions or other results of that search. That motion is the subject of this opinion.

Discussion

In short, Defendant argues that the NIT warrant exceeded the authority of the magistrate in the Eastern District of Virginia and that, as a result, the evidence must be suppressed. Defendant also requests a hearing regarding his allegation that the NIT warrant affidavit contains misleading statements and omissions.

I. Prior Decisions

The Playpen and NIT investigation led to numerous prosecutions around the country, and naturally other defendants have raised similar arguments. Several other judges, including one from this district, have already ruled on the issues, so considering some of those decisions is the sensible place to start.

Of primary interest is the previous decision from this district, and beginning there will provide a framework to understand how the various decisions agree and differ. Judge Pappert of this district denied suppression in *United States v. Werdene*, 188 F. Supp. 3d 431 (E.D. Pa. 2016). He first addressed Federal Rule of Criminal Procedure 41(b), which authorizes magistrate judges to issue warrants in certain circumstances, and found that neither its general grant of authority to issue warrants regarding persons or property within the magistrate's own district, nor its several provisions allowing a magistrate to issue warrants with effect outside his or her own district in certain circumstances, authorized the magistrate to issue the NIT warrant. *Id.* at 440-42. Next, he explained that a Rule 41 violation may be a substantive or constitutional violation on the one hand, or a ministerial or procedural violation on the other. *Id.* at 442. He found that the violation in this instance was not constitutional because there is no reasonable expectation of privacy in an IP address, which, even if not transmitted through all Tor nodes to the endpoint, is voluntarily transmitted to a third party, the first node in the chain. *Id.* at 443-45. He further noted that even if the defendant expected his IP address and identity to remain private because he used Tor for that purpose, society would not consider that expectation reasonable. *Id.* at 445-46. Having concluded that the Rule 41 violation was ministerial rather than constitutional, Judge Pappert noted that in that situation, suppression requires prejudice to the defendant or deliberate disregard of the rule by law enforcement. *Id.* at 446-47. Further noting that the Third Circuit equates prejudice with offense to fundamental fairness or due process, he concluded that the NIT warrant's Rule 41 violation was not prejudicial and suppression was inappropriate; the FBI followed the best procedure it could given the mismatch of Rule 41 and the arrangement of this

particular criminal behavior, and the agents did at least get the approval of a neutral magistrate. *Id.* Finally, Judge Pappert added that even if the violation were in fact constitutional in nature, suppression would not be appropriate because the good-faith exception is available and satisfied in this case; the deterrence value of suppression here, where the mistake was made primarily by the magistrate rather than by law enforcement, does not outweigh the cost of excluding evidence that compellingly demonstrates the defendant's guilt. *Id.* at 447-53.

Only a few cases have found there was no Rule 41 violation. One judge has twice ruled that the magistrate had the authority to issue the warrant because Rule 41 does not expressly prohibit it. *See United States v. Eure*, No. 2:16CR43, 2016 WL 4059663, at *8 (E.D. Va. July 28, 2016); *United States v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016). Other cases found that Rule 41(b)(4), which allows a magistrate to issue a warrant to install a tracking device, authorized the NIT warrant. *See United States v. Jean*, No. 5:15-CR-50087-001, 2016 WL 4771096, at *17 (W.D. Ark. Sept. 13, 2016); *United States v. Matish*, No. 4:16CR16, 2016 WL 3545776, at *24 (E.D. Va. June 23, 2016).

Of the cases finding a Rule 41 violation, a few have granted suppression. Those cases held that because there was no authority to issue the warrant, there was really no warrant at all, and where a warrant is void *ab initio*, there is no good faith exception to the suppression remedy. *See United States v. Croghan*, No. 1:15-CR-48, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); *United States v. Workman*, No. 15-CV-00397-RBJ-1, 2016 WL 5791209 (D. Colo. Sept. 6, 2016); *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016); *United States v. Arterbury*, 15-cr-182 (N.D. Okla. Apr. 25, 2016) (report and recommendation). *Levin*, *Arterbury*, and *Workman* do not directly consider

whether the violation was constitutional, focusing instead on the difference between substantive and merely procedural or technical violations; they find the violation substantive and the defendant prejudiced. *See Workman*, 2016 WL 5791209, at *5 (finding a ruling on constitutional magnitude unnecessary because there was prejudice in any event); *Levin*, 186 F. Supp. 3d at 35-36; *Arterbury*, 15-cr-182, slip op. at 5. *Croghan* follows the void *ab initio* rationale, but also notes that there is a constitutional issue because the third-party doctrine does not cover the circumstances of the NIT investigation; the IP addresses were not obtained from a third party like an ISP or phone company, but rather directly from the suspects' own computers. *See Croghan*, 2016 WL 4992105, at *7.

A number of cases have found a Rule 41 violation but still denied suppression, and their reasoning both diverges and overlaps in several ways. Some largely avoid analysis of whether the violation was constitutional in nature. See *United States v. Allain*, No. 15-CR-10251, 2016 WL 5660452, at *11-12 (D. Mass. Sept. 29, 2016) (stating simply that the technical Rule 41 violation was objectively reasonable and in good faith, and explicitly declining to follow the void *ab initio* reasoning); *United States v. Henderson*, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at *4-5 (N.D. Cal. Sept. 1, 2016) (discussing the constitutional versus technical distinction not as a matter of whether there was a constitutional interest as in *Werdene*, but simply as a matter of whether the violation was serious, answering in the negative because the warrant was properly supported, and finding no prejudice since there is no expectation of privacy for an IP address). In *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016), the court appeared to consider a Rule 41 violation

technical almost by definition, but also noted there was no prejudice to the defendant because he had no expectation of privacy in his IP address, stating that because he sent it out to at least an initial third party it could eventually have been discovered (without explaining how that could have been done).

One decision somewhat mirrors *Werdene*, holding there was no search because the third-party doctrine forecloses any expectation of privacy in an IP address; therefore, even if Rule 41 was violated, the violation was non-constitutional. *See United States v. Acevedo-Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016). The court also applied the good faith exception and denied suppression. *Id.*

A number of others, however, find there was a constitutional issue but apply the good faith exception to deny suppression. They largely reason that even if there is no privacy expectation in IP addresses because they are revealed to third parties, that logic does not apply to this situation because the NIT got the IP address (and other information) directly from the contents of the suspects' computers, in which they do have a reasonable expectation of privacy, rather than from third parties. *See United States v. Anzalone*, No. CR 15-10347-PBS, 2016 WL 5339723, at *6 (D. Mass. Sept. 22, 2016); *United States v. Broy*, No. 16-CR-10030, 2016 WL 5172853, at *5-6 (C.D. Ill. Sept. 21, 2016); *United States v. Ammons*, No. 3:16-CR-00011-TBR-DW, 2016 WL 4926438, at *4 (W.D. Ky. Sept. 14, 2016); *United States v. Knowles*, No. CR 2:15-875-RMG, 2016 WL 6952109, at *8-9 (D.S.C. Sept. 14, 2016); *United States v. Torres*, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3-7 (W.D. Tex. Sept. 9, 2016); *United States v. Ryan Anthony Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *7 (M.D. Fla. Aug. 10, 2016) (also finding the violation so attenuated from the defendant's admissions

and voluntary turnover of evidence months after the warrant was issued that suppression was inappropriate). Some of these found there was a constitutional interest at play and a Fourth Amendment search took place, but held the Rule 41 violation itself was only technical. *See Anzalone*, 2016 WL 5339723, at *6; *Torres*, 2016 WL 4821223, at *3-7; *Ryan Anthony Adams*, 2016 WL 4212079, at *7.

The undersigned will follow Judge Pappert's road map in *Werdene*, considering whether the warrant violated Rule 41, then whether the violation is constitutional in nature, and finally whether suppression is appropriate.

II. Violation of Rule 41(b)

Federal Rule of Criminal Procedure 41(b) allows a magistrate judge to issue a warrant in certain situations. First, "a magistrate judge with authority in the district…has authority to issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). The subsections that follow give limited authority to issue warrants with effect outside the magistrate's jurisdiction: 41(b)(2) covers persons or property in the district when the warrant is issued that might move before execution; 41(b)(3) covers investigations related to terrorism; 41(b)(4) covers installation of tracking devices within the magistrate's district that may subsequently track movement out of the district; and 41(b)(5) covers locations of federal purview outside any district, such as United States territories and United States diplomatic property in other countries. As expected at the time of argument on this motion, and even anticipated to some degree by the government when it applied for the NIT warrant, Rule 41(b) has since gained a new subsection (6), expressly designed for

situations like the one in this case. While the adoption of 41(b)(6) is relevant to assessing this motion in some respects, it was not available to authorize the warrant at the time of its issuance.

Although some cases have found that 41(b)(4), related to tracking devices, authorized the search in this case, the government has not argued here that any of the subsections explicitly authorized the NIT warrant. And although the warrant application was unclear about the place to be searched, referring to deployment of the NIT on the server in Virginia, the information to be seized was clearly located on the various users' computers at their homes outside the magistrate's district. So as the government concedes, none of the subsections empowered the magistrate to issue the NIT warrant. The government argues that the list in 41(b) is not exhaustive, that warrants not expressly authorized may still be permissible, and that the agents here used best efforts to find a judge with a connection to the investigation. The flexibility suggested by the historical approval of pen registers and anticipatory warrants prior to their express inclusion in Rule 41, which the government cites, is not sufficient to allow the warrant here, where the subsections of 41(b) are specifically addressed to the question of warrants having effect outside the magistrate's geographic district. The government's contention that Rule 41 cannot be given an interpretation that would make identifying Tor users impossible is misguided. There are many things the government might wish to do and indeed have public support for that are nevertheless prohibited, and as proven by the subsequent change to Rule 41, the prohibition here was never permanent and insurmountable. So,

like the majority of courts, the undersigned agrees that the NIT warrant was in violation of Rule 41.[1]

III. Constitutional Nature of Rule 41 Violation

In assessing suppression for Rule 41 violations, courts distinguish between constitutional and non-constitutional violations. *See United States v. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988); *Werdene*, 188 F. Supp. 3d at 442. Non-constitutional violations are variously described as "technical," *Martinez-Zayas*, 857 F.2d at 136; *Croghan*, 2016 WL 4992105, at *7; *Levin*, 186 F. Supp. 3d at 35, "ministerial" and "procedural," *Levin*, 186 F. Supp. 3d at 35; *Werdene*, 188 F. Supp. 3d at 442, or simply "not of constitutional import," *Workman*, 2016 WL 5791209, at *5 (quoting *United States v. Krueger*, 809 F.3d 1109, 1114 (10th Cir. 2015). As discussed above, the various prior NIT cases have approached the analysis of this distinction in different ways: some find there was a constitutional interest and Fourth Amendment search but nevertheless find the Rule 41 violation merely technical. The undersigned adopts the approach used in *Werdene* and some of the other cases, which considers a violation constitutional and non-technical if the government action constituted a search under the Fourth. *See, e.g.*, *Ammons*, 2016 WL 4926438, at *3.

Werdene began this analysis from the standpoint that "[t]he Supreme Court of the United States has 'uniformly…held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a "justifiable," a

[1] As to Defendant's contention that a delay in service of the NIT warrant violated Rule 41(f), the government appears to be correct that it secured a series of orders extending the time for service until March 20, 2016 (see Doc. #19 ex. 1). The date Defendant claims the warrant was served, March 7, 2016, is within that time frame.

"reasonable," or a "legitimate expectation of privacy" that has been invaded by the government action.'" 188 F. Supp. 3d at 443 (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (considering the use of a pen register installed at the phone company that records all numbers dialed by a suspect)). The existence of a reasonable expectation of privacy in turn requires both a subjective expectation by the person claiming Fourth Amendment protection and that society be prepared to recognize that expectation as reasonable. *Id.* This approach traces back to *Katz v. United States*, 389 U.S. 347 (1967), which "rejected the argument that a 'search' can occur only when there has been a 'physical intrusion' into a 'constitutionally protected area,' noting that the Fourth Amendment 'protects people, not places.'" *Smith*, 442 U.S. at 739. A corollary to the reasonable expectation of privacy analysis is the third-party doctrine, which holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743–44.

Following the reasonable expectation of privacy analysis and third-party doctrine, *Werdene* noted Third Circuit precedent that held there is no reasonable expectation of privacy in an IP address. *Werdene*, 188 F. Supp. 3d at 443–44 (citing *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010)). Internet users' computers convey IP addresses to outside parties such as ISPs. *Christie*, 624 F.3d at 574. As explained above, even using Tor, a user's IP address is sent to the first node in the relay chain. And under *Smith*, it does not matter that the process is automated and the third party does not ordinarily pay conscious attention to the information. *See Smith*, 442 U.S. at 744-45.

But the ruling in *Christie* is not controlling here. First, it is far from clear that the third-party doctrine really applies in this case, because the FBI did not actually get

Defendant's IP address and other information from a third party. *See United States v. Miller*, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and *conveyed by him to Government authorities*." (emphasis added)); *see also Smith*, 442 U.S. at 745 ("petitioner assumed the risk that the information would be *divulged to police*" (emphasis added)); *Croghan*, 2016 WL 4992105, at *7 (noting that in third-party doctrine precedent, "law enforcement obtained the defendant's IP address *from the defendant's ISP*" (emphasis in original)).

There is also reason to doubt the wisdom of extending the third-party doctrine to new technology, as one member of the Supreme Court has noted:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.

See United States v. Jones, 565 U.S. 400, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted).

Moreover, as a number of the other NIT cases have recognized, the IP address is not the sole focus of the analysis: even if Defendant had no reasonable expectation of privacy in the IP address itself, he may have had such an expectation in his home computer and its contents.[2] *See Anzalone*, 2016 WL 5339723, at *6; *Broy*, 2016 WL 5172853, at *9; *Ammons*, 2016 WL 4926438, at *9; *Knowles*, 2016 WL 6952109, at *10;

[2] As Defendant points out, the government has itself condemned the invasion of personal computers and related theft of personal information in a number of ways. *See, e.g.*, 18 U.S.C.A. § 1030 (criminalizing, among other things, accessing a protected computer without authorization and obtaining information or causing damage by transmitting a program, information, code, or command, where "protected computer" at this point means essentially any computer connected to the internet). In addition to punishing unauthorized computer access, the government has also condoned and recommended use of Tor to protect personal information. *See* Hearing Tr. 2-4, July 28, 2016, *United States v. Bruce Lorente & Gerald Lesan*, Nos. CR15-274RJB & CR15-387RJB (W.D. Wash.) (referring to recommendations of a Department of Justice cybercrime specialist at a seminar for federal judges).

Torres, 2016 WL 4821223, at *7. This is really just another way of noting that the third-party doctrine is inapplicable when the information was not actually obtained from a third party. "[L]aw enforcement caused an NIT to be deployed directly onto Defendants' home computers, which then caused those computers to relay specific information stored on those computers to the Government without Defendants' consent or knowledge. There is a significant difference between obtaining an IP address *from a third party* and obtaining it *directly from a defendant's computer*." *Croghan*, 2016 WL 4992105, at *7. Compare the pen register context: the fact that the numbers a person dials are sent out to a third party and thus entitled to no expectation of privacy does not permit law enforcement to enter a suspect's home and peer over his shoulder while he dials, at least not without a valid warrant. Here, Defendant transmitted his IP address to the first node in the Tor relay, but the FBI used the NIT to look around in Defendant's home computer and get the IP address and other information directly. The undersigned must respectfully diverge from Judge Pappert's analysis and agree with the other NIT decisions that focus the privacy expectation analysis not on the IP address in the abstract, but rather on Defendant's home computer and its contents. In the latter, Defendant had an expectation of privacy that society recognizes as reasonable, given the computer's location inside his home, the widespread use of home computers to store private information, and the criminalization of computer intrusion.

Further, as this focus on Defendant's computer inside his home points up, the *Katz* expectation of privacy analysis is not the sole, universal approach to Fourth Amendment questions. The majority opinion in *Jones* reaffirmed that a straightforward intrusion into private property remains a search in constitutional terms, and the

expectation of privacy approach supplements rather than supplants that basic rule. *See Jones*, 565 U.S. at 404-05 (holding that attachment of a GPS tracker to vehicle was a search, as "[t]he Government physically occupied private property for the purpose of obtaining information"). The Court noted that analysis of this sort of search tracks common-law trespass. *Id.* at 405. Even *Smith* recognized that the *Katz* expectation of privacy analysis applied as an *alternative*; the defendant was merely unable to claim that his own property or constitutionally protected area was invaded because the pen register was installed at the phone company. *See Smith*, 442 U.S. at 741. Here, the data-gathering did take place in Defendant's home. In a legitimate sense—computer code ultimately consists of flipped bits on magnetic storage—the NIT did indeed physically occupy Defendant's computer in his home, and in fact it seized control of his computer and ordered it to send out his identifying information.

Even if one questions whether a computerized search qualifies as a physical intrusion, other Supreme Court precedent has considered the intersection of a *Katz* analysis and a pre-*Jones* simple trespass analysis where high-tech methods were at issue. In *Kyllo v. United States*, the Court held that the use of thermal imaging to detect marijuana grow lamps inside a home constituted a search, reasoning that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use. 533 U.S. 27, 34 (2001). While the NIT is not strictly a "sense-enhancing" technology, it is a new technology, not in general public use, that

allowed agents to discover information they otherwise could not have gotten from outside his home.

Whether under a *Katz* expectation of privacy analysis properly focused on the interest actually invaded (i.e., the home computer rather than the IP address in the abstract) or under an analysis that directly considers the physical or enhanced technological intrusion into Defendant's home, the FBI's use of the NIT did constitute a search under the Fourth Amendment. The government's violation of Rule 41, therefore, is of constitutional dimension.

IV. Appropriateness of Suppression

As *Werdene* went on to point out, however, even though the violation was constitutional in nature, suppression is neither required nor appropriate. *See Werdene*, 188 F. Supp. 3d at 448. Though the Fourth Amendment prohibits unreasonable searches and seizures, suppression of evidence as a remedy for violating that prohibition is not enshrined in the Constitution. *See Davis v. United States*, 564 U.S. 229, 236 (2011); *see also United States v. Katzin*, 769 F.3d 163, 169-70 (3d Cir. 2014). Suppression is not even intended for the benefit of the particular defendant in a given case: "The rule's sole purpose…is to deter future Fourth Amendment violations." *Davis*, 564 U.S. at 236-37. Against the desired deterrent effects of suppression, courts must weigh the unwanted effects of ignoring valuable evidence and, in many cases, letting criminals escape punishment. *See id.* at 237. "For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs." *Id.*

This balance is encapsulated in the good faith exception to suppression. The consequences of doing something wrong cannot very effectively deter someone who does not know he or she is doing anything wrong, so the deterrence value of suppression is low when a government agent has a "reasonable good-faith belief that a search or seizure was in accord with the Fourth Amendment." *United States v. Leon*, 468 U.S. 897, 909, 918-19 (1984) (quoting *Illinois v. Gates*, 462 U.S. 213, 255 (1983) (White, J., concurring in judgment)). The *Leon* good faith exception has developed over many cases. Suppression is inappropriate "[w]here the particular facts of a case indicate that law enforcement officers act[ed] with an objectively reasonable good-faith belief that their conduct [was] lawful, or when their conduct involve[d] only simple, isolated negligence," but it is appropriate where "where law enforcement conduct is deliberate, reckless, or grossly negligent or involves recurring or systemic negligence," or where "a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances." *Katzin*, 769 F.3d at 171 (internal quotation marks omitted). Despite this near-codification of the good faith exception, the point remains to balance deterrence value against the costs of excluding otherwise-valid evidence.

Defendant argues that the good faith exception is simply unavailable in this case because the warrant was void *ab initio*. *See Levin*, 186 F. Supp. 3d at 38-42. It is true that some of the good faith analysis relates to the fact that consideration by a neutral magistrate helps to demonstrate that government agents are acting reasonably and in good faith when they have a warrant. *See Leon*, 468 U.S. at 913-23. But as *Werdene* notes, the Third Circuit has applied the good faith exception when there was no warrant involved at all. *See Katzin*, 769 F.3d at 181-87. Some of the other NIT decisions likewise reject the

reasoning that the good faith exception is foreclosed when the warrant was void *ab initio*. *See Allain*, 2016 WL 5660452, at *11; *Ammons*, 2016 WL 4926438, at *8. The good faith exception is not a rigid or technical rule, nor is it tied to the existence of a warrant; it simply gives form to the basic deterrence-balancing considerations, and there is no reason to hold that suppression is categorically required in this case.

Applying the good faith exception and deterrence-balancing considerations in this case, suppression is not appropriate. Defendant has adamantly argued that the FBI agents acted in bad faith because they concealed or underemphasized the effect of the NIT warrant outside the magistrate's district and because they likely knew there was an ongoing effort to change Rule 41 to specifically allow the warrant they sought (which could imply they knew it was *not* allowed at the time). Defendant also requests a hearing to probe Defendant's allegations of bad faith in this case. *See Franks v. Delaware*, 438 U.S. 154, 156 (1978). But no hearing is necessary. Defendant argues the agents cannot reasonably contend they did not know the NIT would search suspects' computers outside the magistrate's district. This Court agrees, but the very obviousness of this fact means it was also clear to the magistrate. The warrant application mentioned the server located in Virginia in the description of the place to be searched, but it also described the operation of the NIT at length and noted the move from North Carolina to Virginia. The application as a whole did not, and in fact could not, hide from the magistrate that the NIT would target Playpen users without geographic bounds. As for the then-pending efforts to change Rule 41, the agents could have seen that proposed change as merely a clarification of a warrant power the magistrate already had. Even if there was a question,

the agents could reasonably have thought the magistrate herself was better suited to address it and decide it than they were.

Moreover, the subsequent adoption of that rule change certainly highlights the low deterrence value of suppression in this instance. There is always some value in deterring unlawful searches generally, but the particular circumstances of the warrant problems in this case will never arise again. The type of warrant obtained here will be valid in future cases. Even if the new Rule 41 provision were to be changed again, the issue has been and will continue to be the subject of conscious consideration, attention, and litigation, by the courts and perhaps at some point by the legislature, so any future similar warrant application will be made on a very different landscape. That shift, combined with the simple fact that the agents here did indeed apply for and obtain a warrant rather than proceeding without any review, further supports a good faith argument and means that the deterrence value of suppression in this case is extremely low. The costs of suppression, on the other hand, are quite high. The evidence and admissions obtained as a result of the subsequent full search of Defendant's home demonstrate that the identifying information uncovered by the NIT was reliable. The evidence is solid and strongly points to Defendant's guilt of crimes—receipt and possession of child pornography—that our society takes extremely seriously. Excluding the evidence in this case and likely letting Defendant escape conviction for these crimes is a cost that cannot be justified by any minimal deterrent benefit in this case.

Conclusion

In keeping with the vast majority of other decisions involving the same NIT warrant, this Court finds the warrant violated Rule 41. And as concluded in many of those other decisions, there was a constitutional element to the Rule 41 violation because the government did not obtain Defendant's IP address and other information from a third party, but rather searched and even seized control of his home computer. Nevertheless, not all Fourth Amendment violations require suppression. The agents here acted in good faith. Given the high cost of excluding the evidence at issue here and the limited opportunity to deter government conduct where Rule 41 has changed and the same circumstances will not arise in the future, suppression is not appropriate. Defendant's motion is accordingly denied.